Migration to E-Authentication

August 2004

egov

My Government. My Terms.

Steps for Implementing E-Authentication

1. Conduct an authentication requirements analysis and risk assessment for the e-government application
2. Map identified risks to the applicable assurance level
3. Select technology based on E-Authentication technical guidance
4. Implement the solution and validate that the implemented application has achieved the required assurance level
5. Periodically reassess the system to determine technology refresh requirements

And the E-Authentication PMO can help!

Prerequisites

If your application has already been developed, each of the following (as they apply to your application) should either be completed, or planned to be completed, prior to fully implementing E-Authentication:

1. Privacy Impact Assessment (PIA)
2. Authorization to Operate (C&A)
3. 508 Compliant
4. Exhibit 300 Scored and Approved

Step One

- **The Task**: Conduct an authentication requirements and risk assessment for the e-government application
- **The Process**: Use an approved risk assessment methodology. The **E-RA tool** and guidance, provided by E-Authentication, have been specifically developed to map to the levels of assurance defined in guidance released by OMB. The E-RA tool systematically assesses the impact of inconvenience, distress or damage to standing or reputation; financial loss; harm to agency programs or public interests; unauthorized release of sensitive information; personal safety; civil or criminal violations
- **Points of Note**:
  - An application may have multiple categories or types of transaction, which may require different assurance levels
  - Risk assessment is a subjective process
  - If the application collects personal information, then the agency must develop and submit a system of records notice
  - Also, to comply with privacy regulations (e.g. the E-Gov Act of 2002), the agency should perform a Privacy Impact Assessment (PIA)

Step One – (Continued)

- **Reference Documents**:
  - A-130, Section 5 of OMB Government Paperwork Elimination Act (GPEA) Guidance
  - E-Authentication Guidance for Federal Agencies (OMB M04-04)
  - The Privacy Act of 1974
  - The E-Government Act of 2002
- **E-Authentication Documents**:
  - E-Authentication Handbook for Federal Government Agencies
  - The Electronic Risk and Requirements Assessment (E-RA tool)
  - E-RA Assessment Guide
- **PMO Services**:
  - Assistance in how to use the E-RA tool
  - How to interpret E-Authentication policy and guidance

Step Two

- **The Task**: Map identified risks to the required assurance level as defined in OMB's assurance level guidance (E-Authentication Guidance for Federal Agencies, OMB M04-04)
- **The Process**: Refer to the E-RA tool and guidance, for each impact category, based on the potential low, moderate or high impact, use the impact profile guide to determine the appropriate level of assurance (1-4)
- **Points of Note**:
  - Tie the potential impact category outcomes to the authentication level, choosing the lowest level of authentication that will cover all of the potential impacts identified
  - Identify risks inherent in the transaction process, regardless of its authentication technology

Step Two – (Continued)

- **Reference Documents**:
  - A-130, Section 5 of OMB GPEA Guidance
  - E-Authentication Guidance for Federal Agencies (OMB M04-04)
- **E-Authentication Documents**:
  - E-Authentication Handbook for Federal Agencies
  - The Electronic Risk and Requirements Assessment (E-RA tool)
  - E-RA Assessment Guide
- **PMO Services**:
  - Assistance in how to use the E-RA tool
  - How to interpret E-Authentication policy and guidance

Step Three

- **The Task**: Select technology based on the NIST E-Authentication technical guidance (Electronic Authentication Guideline, NIST SP 800-63)
- **The Process**:
  - Refer to the results of the E-RA and both the OMB M04-04 and the E-Authentication Handbook for Federal Agencies to determine an acceptable method of authentication and to develop the architecture
  - Execute MOU/MOA with E-Authentication PMO
  - If your application requires level 1 or 2 assurance, refer to the Approved E-Authentication Technology Provider List to select components
  - If your application requires level 3 or 4 assurance, contact the E-Authentication PMO to develop a PKI implementation plan
- **Points of Note**:
  - After determining the assurance level, refer to NIST SP800-63 to identify and implement the appropriate technical requirements
  - NIST SP 800-63 is the foundation for the Credential Assessment Framework (CAF), used to determine the trustworthiness of electronic/digital identity credentials

Step Three – (Continued)

- **Reference Documents**:
  - E-Authentication Guidance for Federal Agencies (OMB M04-04)
  - Electronic Authentication Guideline (NIST SP800-63)
- **E-Authentication Documents**:
  - E-Authentication Handbook for Federal Agencies
  - E-Authentication Cookbook
  - The E-Authentication Technical Architecture
  - Trusted Credential Service Provider List
  - The Electronic Risk and Requirements Assessment (E-RA tool) & Guide
  - E-Authentication Credential Assessment Suite
- **PMO Services**:
  - Guidance on the selection of E-Authentication technology and the implementation of the architecture
  - To integrate an agency application with the E-Authentication architecture, a Memorandum Of Understanding (MOU), if the PMO provides funding, or a Memorandum Of Agreement (MOA), if no funding is required, will be executed to document the agreed upon responsibilities and desired outcomes.
    - MOU/MOA Contains: Required GSA actions, Required Agency actions, proposed schedule and milestones and measures of success. For MOUs only: Funding requirements, timing and source.

Step Four

- **The Task**: Implement the E-Authentication solution and then validate that the application has operationally achieved the required assurance level
- **The Process**:
  - For implementation, reference the E-Authentication Cookbook and Interface Specifications for guidance on how to implement the E-Authentication architecture and integrate the components into the agency environment.
  - Then contact the E-Authentication PMO to schedule application interoperability testing with the E-Authentication Interoperability Lab.
  - Finally, reference the Validation Checklist for assistance on the validation process and how to successfully complete the certification and accreditation processes.

Step Four – (Continued)

- **Points of Note**:
  - This validation process should be part of the agency's required security procedures (e.g. certification and accreditation)
- **Reference Documents**:
  - E-Authentication Guidance for Federal Agencies (OMB M04-04)
  - Electronic Authentication Guideline (NIST SP800-63)
- **E-Authentication Documents**:
  - E-Authentication Handbook for Federal Agencies
  - E-Authentication Cookbook
  - Interface Specifications
  - Validation Checklist
- **PMO Services**:
  - Technical guidance relative to the validation of the E-Authentication solution
  - Assistance in the validation process

Step Five

- **The Task**: Periodically reassess the application to determine technology refresh requirements
- **The Process**:
  - Refer to the E-Authentication Cookbook and E-Authentication Handbook for Federal Agencies, as well as the Validation Checklist and E-Authentication newsletters to verify that the E-Authentication process is working as required
  - Also determine if any changes in capability, architecture, components, and/or Credential Service Providers (CSP) is necessary
- **Points of Note**:
  - Agencies may adjust the level of assurance using additional risk mitigation measures
  - Reassessment should be part of ongoing Federal Information Security Management Act (FISMA) compliance procedures

Step Five – (Continued)

- **Reference Documents**:
  - E-Authentication Guidance for Federal Agencies (OMB M04-04)
  - Electronic Authentication Guideline (NIST SP800-63)
- **E-Authentication Documents**:
  - E-Authentication Handbook for Federal Agencies
  - E-Authentication Cookbook
  - Interface Specifications
  - Validation Checklist
- **PMO Services**:
  - Technical guidance relative to the reassessment of the E-Authentication solution
  - Assistance in determining if a technology refresh may be required

Reference Documents

- A-130, Section 5 of OMB GPEA Guidance
  http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html
  Or
  http://www.whitehouse.gov/omb/circulars/a130/a130trans4.pdf

- E-Authentication Guidance for Federal Agencies (OMB M04-04)
  http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf

- Electronic Authentication Guideline (NIST SP800-63)
  http://www.cio.gov/eauthentication/documents/SP800-63V6_3_3.pdf

- The Privacy Act of 1974
  http://www.copyright.gov/fedreg/1999/64fr54361.html

- The E-Government Act of 2002
  http://csrc.nist.gov/policies/HR2458-final.pdf

E-Authentication Documents/Tools

Documents

- The E-Authentication Technical Architecture:
  - Technical approach for the E-Authentication Service Component
    http://www.cio.gov/eauthentication/documents/TechApproach.pdf
  - SAML Artifact Profile as an Adopted Scheme for E-Authentication
    http://www.cio.gov/eauthentication/documents/SamlArtifactAdoptedScheme.pdf
  - E-Authentication Interface Specifications for the SAML Artifact Profile
    http://www.cio.gov/eauthentication/documents/SamlSpecs.pdf

- Trusted Credential Service Provider List
  - http://www.cio.gov/eauthentication/documents/TCSP.pdf

- Approved E-Authentication Technology Provider List
  - http://www.cio.gov/eauthentication/documents/ApprovedProviders.htm

- E-Authentication Handbook for Federal Agencies
  - http://www.cio.gov/eauthentication/documents/GOVhandbook.pdf

E-Authentication Documents/Tools (cont.)

Documents (cont.)

- E-Authentication Cookbook
  http://www.cio.gov/eauthentication/documents/Cookbook.pdf

- Validation Checklist – TBD

- E-Authentication Risk & Requirements Assessment Guide
  http://www.cio.gov/eauthentication/documents/eraguide.pdf

- CAF Guidance
  http://www.cio.gov/eauthentication/documents/CAG.pdf

Tools

- E-Authentication Risk & Requirements Assessment (E-RA tool)
  http://www.cio.gov/eauthentication/era.htm

- CAF
  http://www.cio.gov/eauthentication/documents/CAF.pdf

E-Auth Documents: Agency Handbook

- E-Authentication Handbook for Federal Agencies
  - Serves as an agency guide on how to implement E-Authentication
  - Topics include how to “E-Authenticate” an agency application, implementation guidance, operational responsibilities, maintenance and technical evolution, and resources

E-Auth Documents: E-Authentication Cookbook

- The E-Authentication Cookbook can assist agencies in migrating applications and credential services to the E-Authentication framework
- It addresses **various scenarios**, with more scenarios supported as more implementations occur
- Each Cookbook entry contains **step-by-step "recipes"** with detailed instructions
- Categories of recipes include:
  - Processes
  - Integration
  - Implementation
  - Products and services

E-Auth Documents: E-Authentication Cookbook

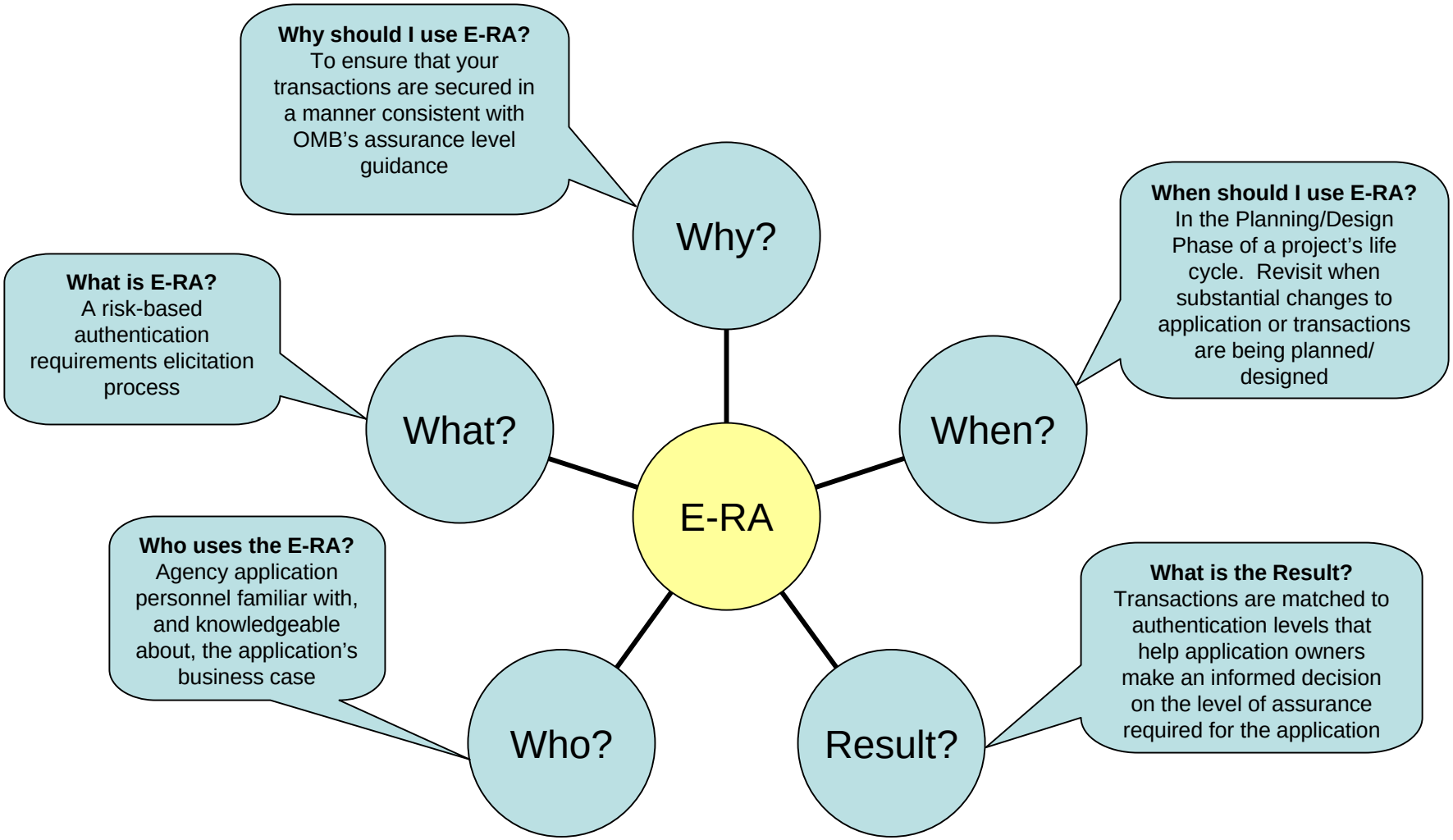
Examples of Cookbook recipes:

- Request to obtain Public Key Infrastructure (PKI) credentials
- Obtaining an agency application ID
- Obtaining a Credential Service ID
- Browser requirements and authentication
- Browser and Server Certificates
- Integration testing
- Importing browser and server certificates
- Certificate revocation list verification and timelines
- Redirecting users to the E-Authentication portal

E-Auth Document: The Validation Checklist

- Initial Validation
  - Agencies may use the resources at the Interoperability Lab to perform conformance and interoperability testing of their applications with installed E-Authentication products and services
- Recurring Validation
  - Also, in development, is a checklist that agencies can use to perform periodic validation of the E-Authentication process
  - This Validation Checklist can also support FISMA processes and reporting

E-Auth Tools: E-RA (The Basics)



E-Auth Tools: E-RA (The Timing)

How can an agency determine if it is ready to do an E-RA on an application?

1. The purpose of the application has been defined
2. The “To Be Transactions” have been defined, including users/actors and types of data involved

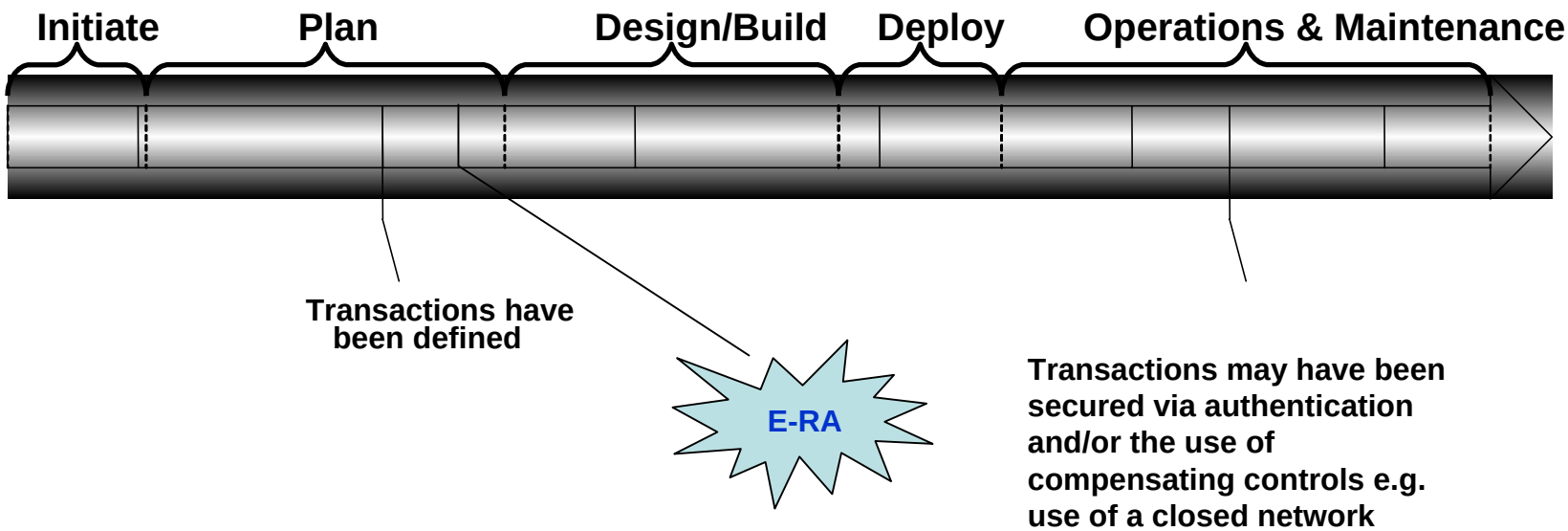
E-Auth Tools: E-RA Transaction Requirements

What does an agency need to know about its transactions?

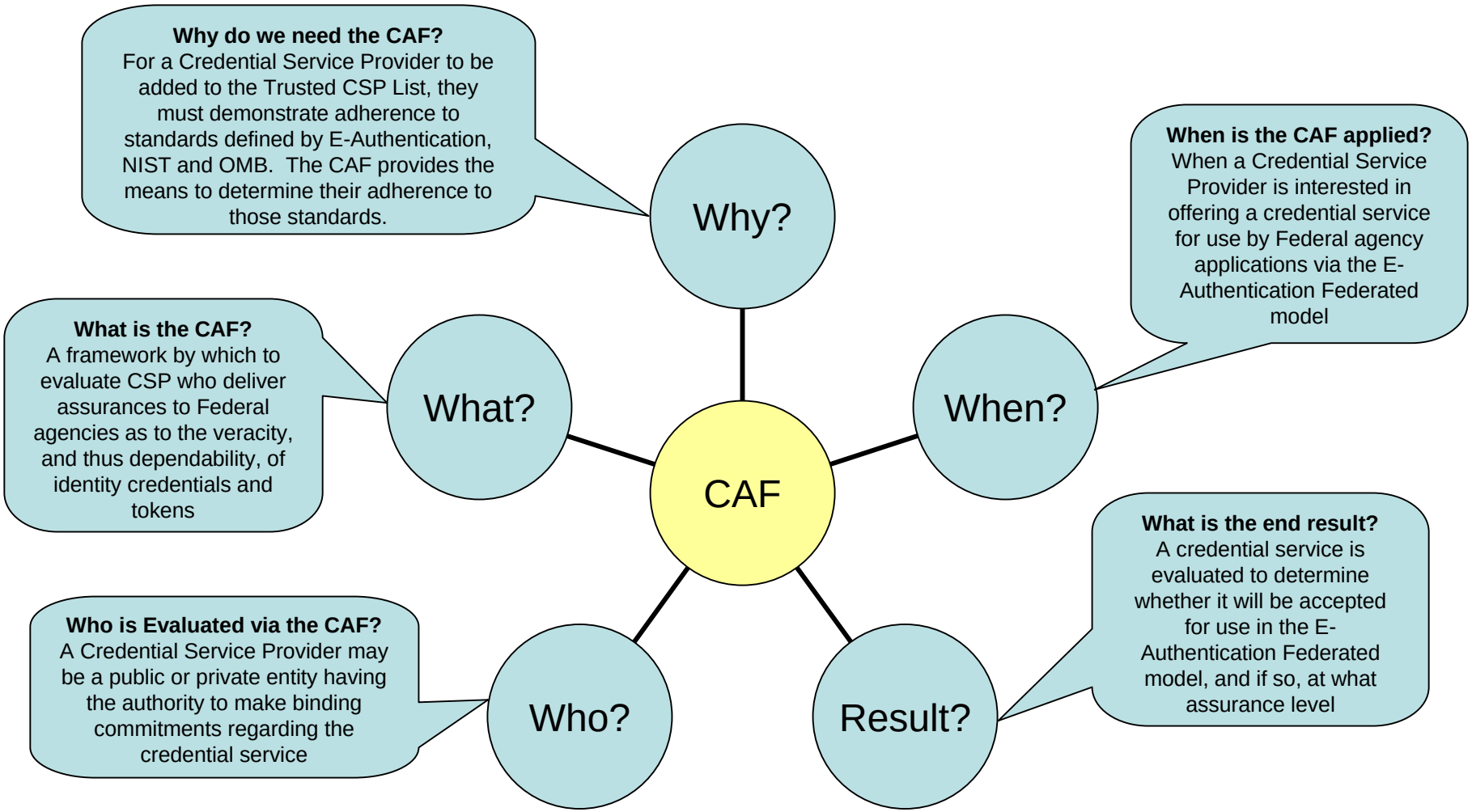
1. Know the structure of the transactions, who can use them and what is expected to happen when they are used
2. Be able to identify the following types of transactions:
   - Critical – most relevant transactions
   - Common – those transactions used most frequently
   - Range – upper and lower limits of functionality allowed
   - Type – Inquire, Create, Modify, Delete
3. Know the security requirements of information in the transactions
4. Be able to identify potential impacts to the organization, customer, vendors and partners

E-Auth Tools – E-RA (in a Project Lifecycle)

Where in a Project life cycle is the E-RA performed?



E-Auth Tools: Credential Assessment Framework (CAF) The Basics



For More Information

Sharon Terango 703-872-8619 sharon.terango@gsa.gov
Lead Agency Manager

Myisha Frazier-McElveen 703-872-8626 myisha.frazier-mcelveen@gsa.gov
Agency Manager

Websites

http://cio.gov/eauthentication
http://www.cio.gov/ficc/
http://cio.gov/fpkipa